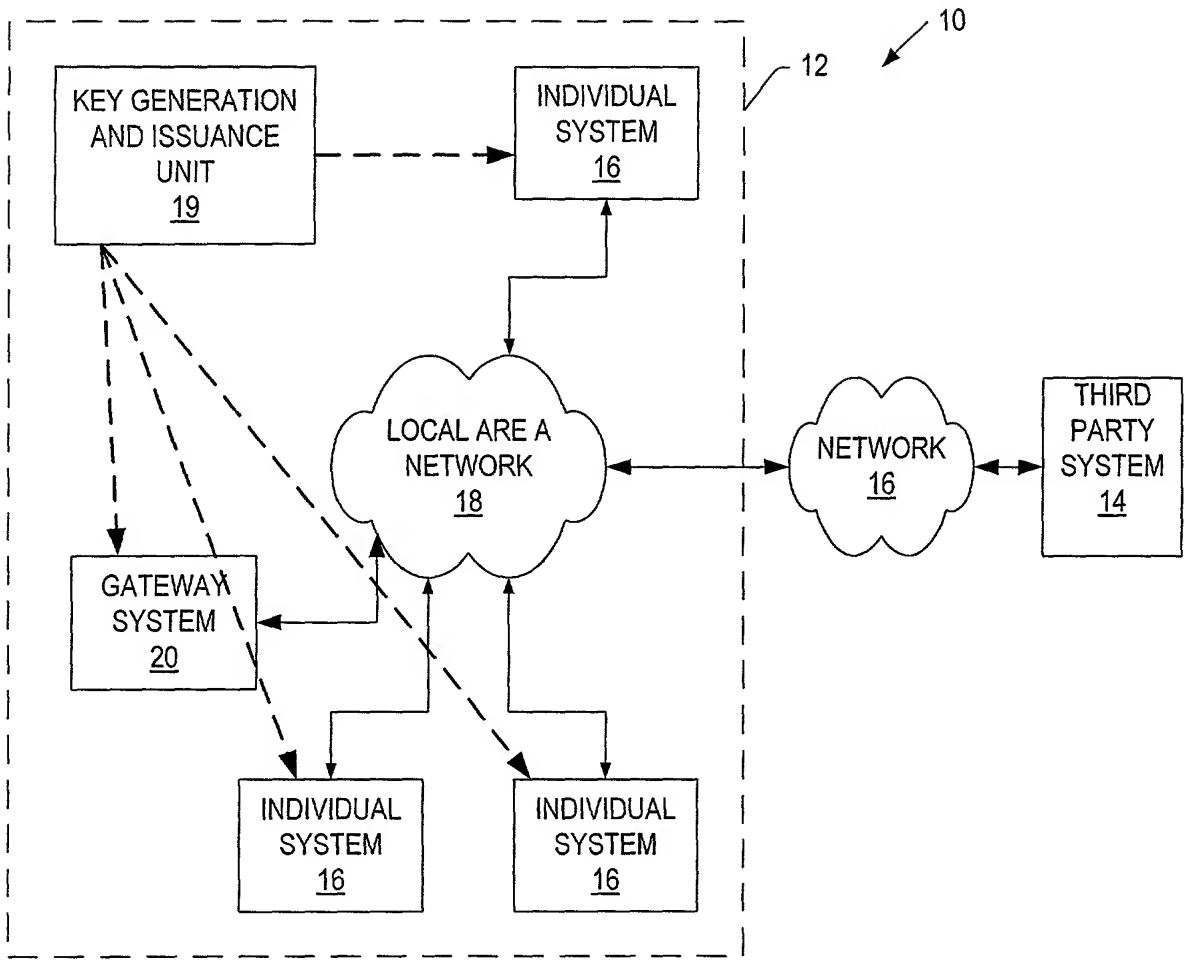
10
12
KEY GENERATION AND ISSUANCE UNIT 19
INDIVIDUAL SYSTEM 16
LOCAL ARE A NETWORK 18
NETWORK 16
THIRD PARTY SYSTEM 14
GATEWAY SYSTEM 20
INDIVIDUAL SYSTEM 16
INDIVIDUAL SYSTEM 16

FIG. 1

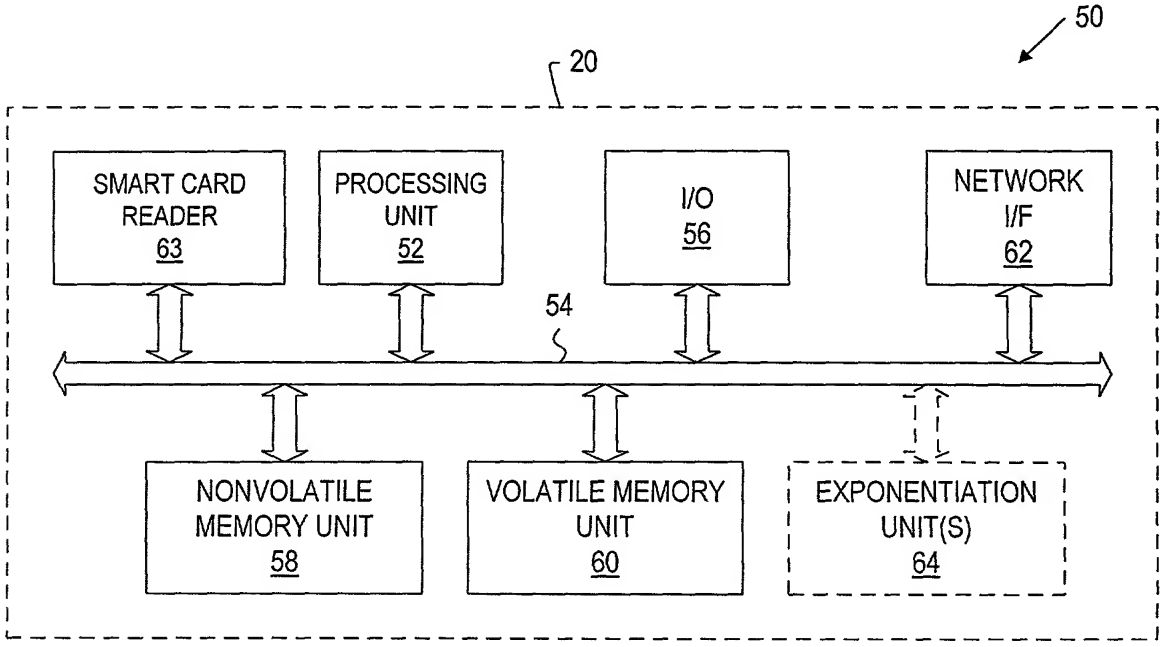
50
20
SMART CARD READER 63
PROCESSING UNIT 52
I/O 56
NETWORK I/F 62
54
NONVOLATILE MEMORY UNIT 58
VOLATILE MEMORY UNIT 60
EXPONENTIATION UNIT(S) 64

FIG. 2

60

INDIVIDUAL OF GROUP	GROUP_1	GROUP_2	GROUP_3	GROUP_4	GROUP_5
INDIVIDUAL_1	$n_{11}=p_1p_6$	$n_{21}=p_1p_2$	$n_{31}=p_1p_4$	$n_{41}=p_1p_5$	$n_{51}=p_1p_3$
INDIVIDUAL_2	$n_{12}=p_2p_3$	$n_{22}=p_3p_4$	$n_{32}=p_2p_6$	$n_{42}=p_3p_6$	$n_{52}=p_4p_6$
INDIVIDUAL_3	$n_{13}=p_4p_5$	$n_{23}=p_5p_6$	$n_{33}=p_3p_5$	$n_{43}=p_2p_4$	$n_{53}=p_5p_2$

FIG. 3

70

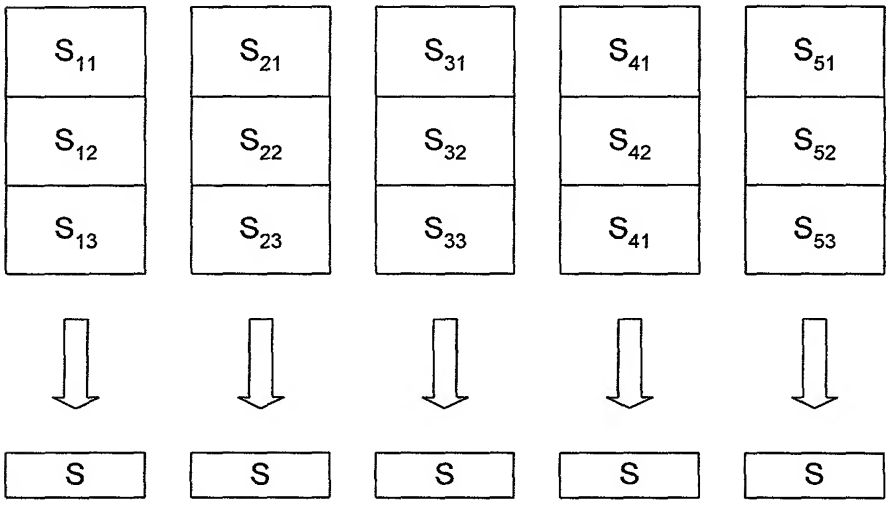

FIG. 4

80

k = 3

INDIVIDUAL #	GROUP_1	GROUP_2	GROUP_3
INDIVIDUAL_1	$n_{11}=p_1$	$n_{21}=p_2$	$n_{31}=p_3$
INDIVIDUAL_2	$n_{12}=p_2p_3$	$n_{22}=p_1p_3$	$n_{32}=p_1p_2$

FIG. 5

90

k = 5

INDIVIDUAL #	GROUP_1	GROUP_2
INDIVIDUAL_1	$n_{11}=p_1$, $n_{21}=p_1$	
INDIVIDUAL_2	$n_{12}=p_2p_3$	$n_{22}=p_2p_4$
INDIVIDUAL_3	$n_{13}=p_4p_5$	$n_{23}=p_3p_4$

FIG. 6

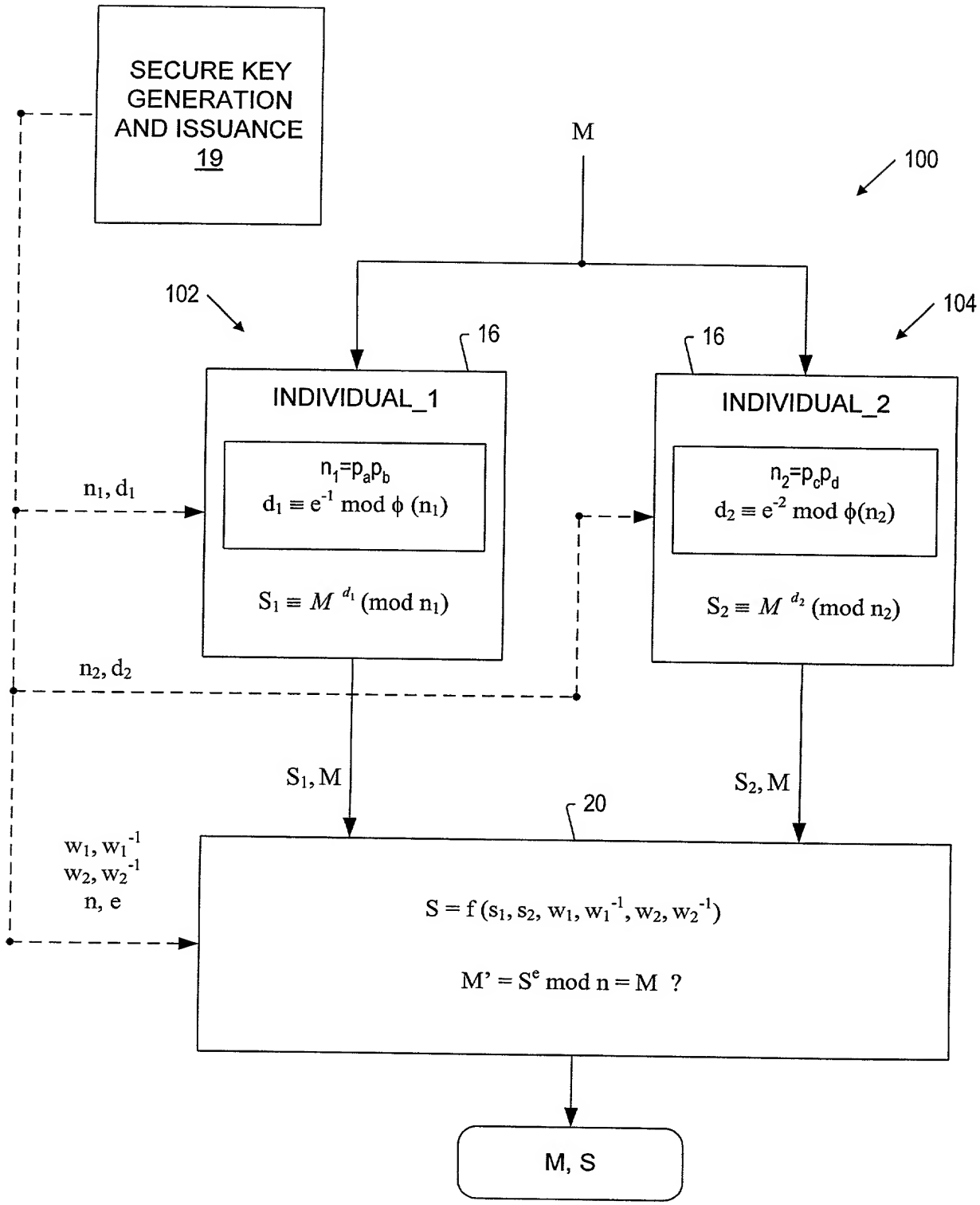
SECURE KEY GENERATION AND ISSUANCE 19
M
100
102
104
16
16
INDIVIDUAL_1
INDIVIDUAL_2
$n_1=p_ap_b$
$d_1 \equiv e^{-1} \bmod \phi(n_1)$
$S_1 \equiv M^{d_1} \pmod{n_1}$
$n_2=p_cp_d$
$d_2 \equiv e^{-2} \bmod \phi(n_2)$
$S_2 \equiv M^{d_2} \pmod{n_2}$
n_1, d_1
n_2, d_2
S_1, M
S_2, M
20
w_1, w_1^{-1}
w_2, w_2^{-1}
n, e
$S = f(s_1, s_2, w_1, w_1^{-1}, w_2, w_2^{-1})$
$M' = S^e \bmod n = M$?
M, S

FIG. 7